



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,752	09/12/2002	Mohamed Khalil	22171-321	2811

7590 10/27/2006
Bill R Naifeh
Haynes and Boone
901 Main Street Suite 3100
Dallas, TX 75202-9918

EXAMINER

TRAN, ELLEN C

ART UNIT PAPER NUMBER

2134

DATE MAILED: 10/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/089,752

Applicant(s)

KHALIL ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 August 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 16-30 and 70-75 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 16-30 and 70-75 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responsive to communication: an original application filed 12 September 2002, with acknowledgement of continuing data from a 317 of PCT/US00/27352 filed 4 October 2000, with a provisional application filed 5 October 1999.
2. Due to preliminary amendment Claims 16-30 and 70-75 are currently pending in this application, claims 1-15, 31-69, and 76-127 have been cancelled. Claims 16 and 70 are independent claims. Claim 70 has been amended, amendment to the claim is accepted.

Response to Arguments

3. The objections made in the previous Office Action to the abstract and claims are removed due to amendment and arguments submitted.
4. Applicant's arguments with respect to claim 16-30 and 70-75 filed 15 August 2006 have been fully considered but they are not persuasive.

Brief summary of prior art of records:

Tisdale: discloses an authentication system for mobile communications in which encryption keys are changeable at the mobile earth terminal (MET), through any known key distribution system see col. 8, lines 36-38.

Chuah: discloses a wireless data network with an optimum routing system (see Abstract).

Cheng: discloses a radio telecommunications system that minimizes the time needed to use a security association (see Abstract).

Inoue: discloses a mobile IP communications scheme for supporting mobile computers (see Abstract).

In response to applicant's argument on beginning on page 7, "However neither Inoue nor Tisdale disclose "the home domain receiving and processing the registration request to generate a registration reply comprising or more encryption keys ... Applicant submits that Tisdale fails to cure this deficiency ... Thus, Tisdale does not disclose generating a registration reply "comprising one or more encryption keys for encrypting messages". The Examiner disagrees with applicant's arguments for multiple reasons. One it is noted the applicant is arguing the references individually where it is the combination that was used in the Office Action. Inoue teaches generating a registration reply and Tisdale teaches distributing encryption keys. Second Tisdale does teach distributing encryption keys, Tisdale merely indicates in the passage cited that these keys are not transmitted in the clear but rather encrypted, see col. 9, lines 49-56, or calculated by the MET based on received signals see col. 10, line 61 through col. 12, line 47.

In response to applicant's argument on page 9, "Prior art teaches away from the claims cannot be used to establish obviousness". Again the Examiner disagrees with this argument, and notes that Tisdale teaches numerous methods of distributing encryption keys.

In response to applicant's argument beginning on page 10, "Applicant respectfully traverses this rejection on the grounds that the references are defective in establishing a prima facie case of obviousness with respect to amended claim 70 ... neither Chuah nor Cheng discloses "dynamically establishing a security association between the initiator and the responder, whereby the initiator presents to the responder a registration request that includes one or more proposals". The Examiner disagrees with applicant's argument and notes the amended claim was not presented in the original presentation; therefore no previous rejection was provided. The below rejection shows that the one or more proposals is taught in Chuah see

Art Unit: 2134

col. 21, lines 46-62 that teaches that the initiator has a user profile inherently is providing one or more proposals.

In response to applicant's argument on page 11, "Chuah does not disclose "dynamically establishing a security association between the initiator and the responder." Applicant submits that Cheng fails to cure this deficiency". The Examiner disagrees with argument Cheng teaches dynamically establishing a security association see col. 2, lines 9-17 note dynamically is an obvious variation of quickly therefore the already negotiated security associations reused allow for quick negotiations between initiator and responder.

In response to applicant's argument beginning on page 12, "The combination of references is improper ... whereby the initiator presents to the responder a registration request that includes one or more proposals. The Examiner disagrees as stated above Chuah does disclose the initiator proposing alternatives with the established profiles. The motivation to combine the two references was established in previous Office Action, which is repeated below to save time when a mobile unit moves from one access point to another see '130 col. 1, lines 61 et seq.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 70-75** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chuah et al. U.S. Patent No. 6,400,722 (hereinafter '722) in further view of Cheng et al. U.S. Patent No. 6,418,130 (hereinafter '130).

As to independent claim 70, "A method of providing secure communications between an initiator and a responder in a communications network, comprising:" is taught in '722 col. 5, lines 1-43 (note the initiator is interpreted to be the end users with remote wireless access, the secure communications is interpreted to be the private intranets, the responder is network being communicated to);

"whereby the initiator presents to the responder a registration request that includes one or more proposals" is shown in col. 21, lines 46-62, note the subscriber's service profile inherently is a registration request that includes one or more proposals; the following is not taught in '722: **"dynamically establishing a security association between the initiator and the responder"** however '130 teaches "It is an object of the present invention to provide a technique which improves the performance of a mobile unit (MU) in a wireless LAN or mobile IP environment, particularly during hand-over. The present invention accomplishes this by reusing rather than renegotiating the security associations (SAs) corresponding to the MU once the MU is handed-over. By reusing the SAs, less time is spent negotiating SAs. Consequently, a MU can begin secure communications almost immediately upon being handed-over from one SU to a another SU" in col. 2, lines 9-17" (note dynamically is interpreted to have the same meaning as immediately).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '722 a mobile communication scheme to include a means to

Art Unit: 2134

dynamically set Security Associations (SA) as taught in '130. One in the art would have been motivated to perform such a modification because as indicated by '130 a need exist to improve the SAs so that they do not have to be renegotiated each time a mobile unit moves from one access point to another (see '130 col. 1, lines 61 et seq.) "Because the SAs (i.e., the ISAKMP SA and the IP_{SEC} SAs) are bound to the negotiating parties, the SAs are renegotiated whenever a mobile unit moves from one access point to another in a wireless LAN environment, or from one foreign agent to another in a mobile IP context. However, the IKE negotiation process is computationally intensive, particularly phase 1. This is especially troublesome in wireless LAN and mobile IP applications where the mobile unit is frequently undergoing hand-over from one SU to another and where the MU has limited computational power. Under such conditions, overall system performance will be exceptionally low since a significant amount of time must be spent renegotiating SAs rather than communicating".

As to dependent 71, "further comprising: negotiating the security association" is disclosed in '722 col. 26, lines 7-48.

As to dependent 72, "wherein negotiating the security association comprises: negotiating one or more security transforms to be used to provide secure communications between the initiator and the responder" is disclosed in '722 col. 26, lines 23-43 (note the User name and the security parameter index (SPI) is specified in the registration message, the User name and the SPI defines the security associations).

As to dependent 73, "wherein negotiating the security association comprises: proposing the number of transforms to be used to provide secure communications between the initiator and the responder" is taught in '722 col. 26, lines 23-43.

As to dependent 74, “wherein negotiating the security association comprises: proposing the duration of at least a portion of the security association” is shown in ‘130 col. 6, lines 26-44 (note lifetime is interpreted to have the same meaning as duration) “FIG. 3 illustrates, more specifically, the SA attributes that might be transferred from $SU_{sub.k}$ to SU_{k+1} , if the partial SA reuse embodiment is employed. As illustrated, SU_k 105, upon receiving a SA request message from SU_{k+1} 110, as indicated by the directional arrow marked “2”, sends a reply message 305 to SU_{k+1} 110, wherein the reply message 305 contains the information necessary to define the following ISAKMP SA attributes: the ISAKMP SA lifetime; the ISAKMP session keys, including the ISAKMP session key for authentication and the ISAKMP session key for encryption; keying material, which is required for deriving the IP_{SEC} session keys; the last IKE phase 1 CBC (i.e., cipher block chaining) output block for generating an initialization vector which, in turn, is needed for the encryption of the first IKE phase 2 message”.

As to dependent 75, “wherein negotiating the security association comprises: proposing the type of transforms to be used to provide secure communications between the initiator and the responder” is disclosed in ‘722 col. 26, lines 23-43.

7. **Claims 16-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Inoue U.S. Patent No. 6,501,767 (hereinafter ‘767) in further view of Tisdale et al. U.S. Patent No. 5,708,716 (hereinafter ‘716).

As to independent claim 16, “A method of providing secure communication between a mobile node and a home domain using a foreign domain comprising:” is taught in ‘767 col. 4, lines 29-45;

“transmitting a registration request from the mobile node to the home domain the request comprising an identity of a user of the mobile node in encrypted form and network routing information in non-encrypted form” is shown in ‘767 col. 9, lines 39-48 (note see FIG. 5, which indicates the shaded portion is encrypted);

“the home domain relaying and processing the registration request to generate a registration reply” is disclosed in ‘767 col. 4, line 63 through col. 5, line 10;

“and transmitting the registration reply from the home domain to the foreign domain and the mobile node” is taught in ‘767 col. 9, line 40 through col. 10, line 43; the following is not taught in ‘767: **“comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node home”** however ‘716 teaches “It is another feature and advantage of the satellite communication system to provide a fraud detection and user validation system where keys are not transmitted “over the air” in the clear. It is another feature and advantage of the satellite communication system to provide a fraud detection and user validation system where the keys are changeable at the MET ” in col. 7, line 63 through col. 8, line 3.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of ‘767 a mobile communication scheme to include a means to generate a reply that utilizes one or more encryption keys as taught in ‘716. One in the art would have been motivated to perform such a modification because as indicated by ‘767 “Here, either this common key is shared between nodes in advance, or a procedure for key sharing between nodes is carried out when the need arises”, in col. 8, lines 13-20. Also as indicated by ‘716 a need exists for a mobile terminal system where keys can be changed (see ‘716 col. 7, lines 21 et seq.)

“It is also desirable to provide a fraud detection and user validation system where transmitted authorization/validation is variable with each call setup to preclude fraudulent reuse”.

As to dependent claim 17, “wherein transmitting a registration request from the mobile node to the home domain comprises: transmitting the registration request from the mobile node to the foreign domain, and transmitting the registration request from the foreign domain to the home domain” is taught in ‘767 col. 4, line 54 through col. 5, line 9.

As to dependent 18, “wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the foreign domain and the home domain” is shown in ‘767 col. 8, lines 13-19.

As to dependent 19, “wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the foreign domain and the mobile node” is disclosed in ‘767 col. 8, lines 20-38.

As to dependent 20, “wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the home domain and the mobile node” is taught in ‘767 col. 8, lines 20-38.

As to dependent 21, “wherein processing the registration request from the mobile node within the home domain comprises decrypting the encrypted form of the identity of the user” is shown in ‘767 col. 9, lines 10-23.

As to dependent 22, “wherein generating a registration reply comprises encrypting at least one of the encryption keys” is disclosed in ‘716 col. 11, lines 14-35. The motivation to combine ‘716 and ‘767 is the same as stated above in claim 16.

As to dependent 23, “wherein generating a registration reply comprises encrypting the encryption keys for encrypting messages to be communicated between the mobile node and me home domain, and between the mobile node and the foreign domain” is taught in ‘767 col. 4, line 63 through col. 5, line 10.

As to dependent 24, “ further comprising: decrypting one or more of the encrypted encryption keys” is shown in ‘716 col. 11, lines 10-35. The motivation to combine ‘716 and ‘767 is the same as stated above in claim 16.

As to dependent 25, “wherein generating the registration reply comprises: generating a first encryption key for encrypting messages to be communicated between the mobile node and the home domain, generating a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain, and generating a third encryption key for encrypting messages to be communicated between the foreign domain and the mobile node” is disclosed in ‘716 col. 11, lines 10-35 and ‘767 col. 8, lines 13-19. The motivation to combine ‘716 and ‘767 is the same as stated above in claim 16.

As to dependent 26, “wherein generating the registration reply comprises encrypting at least one of the first an: third encryption keys” is taught in ‘716 col. 11, lines 10-35. The motivation to combine ‘716 and ‘767 is the same as stated above in claim 16.

As to dependent 27, “further comprising: decrypting at least one of the encrypted first and third encryption keys” is shown in ‘716 col. 11, lines 10-35. The motivation to combine ‘716 and ‘767 is the same as stated above in claim 16.

As to dependent 28, “wherein the registration reply includes encryption keys that are encrypted” is disclosed in ‘716 col. 11, lines 10-35;

“and encryption keys that are not encrypted” is taught in ‘716 col. 9, lines 13-17, ‘716 col. 19, lines 47-65, as well as ‘767 col. 9, lines 39-49 (Note although ‘716 indicates that it does not transmit encryption keys in the clear, the encryption key can be determined from information provided unencrypted in the registration message such as identifiers shown in both ‘716 and ‘767, these identifiers are interpreted to be equivalent to encryption keys that are not encrypted). The motivation to combine ‘716 and ‘767 is the same as stated above in claim 16.

As to dependent 29, “further including: extracting one or more of the encryption keys that are not encrypted from the registration reply” is disclosed in ‘767 col. 10, lines 15-43 (Note as shown in FIG. 5 the unshaded portion is not encrypted).

As to dependent 30, “further including: extracting and decrypting one or more of the encryption keys that are encrypted from the registration reply” is taught in ‘767 col. 10, lines 15-43.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Art Unit: 2134

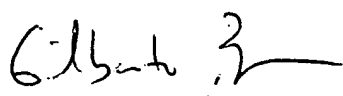
8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is

(571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT
Ellen. Tran
Patent Examiner
Technology Center 2134
20 October 2006


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100